



RECEIVED

MAY 31 2001

071179

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 4月 4日

出願番号

Application Number:

特願2000-102702

出願人

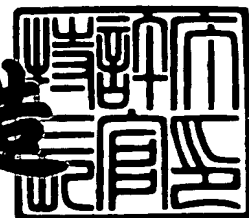
Applicant(s):

富士通株式会社

2001年 4月27日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3035066

【書類名】 特許願

【整理番号】 9951649

【提出日】 平成12年 4月 4日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/22
H04L 12/24

【発明の名称】 通信データ中継装置

【請求項の数】 3

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 小口 直樹

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089244

【弁理士】

【氏名又は名称】 遠山 勉

【選任した代理人】

【識別番号】 100090516

【弁理士】

【氏名又は名称】 松倉 秀実

【連絡先】 03-3669-6571

【手数料の表示】

【予納台帳番号】 012092

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

特 2 0 0 0 - 1 0 2 7 0 2

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705606

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信データ中継装置

【特許請求の範囲】

【請求項 1】 1 以上のネットワークからなる、そのような 2 以上のドメイン間を中継する通信データ中継装置であって、中継元のドメインが中継先のドメインへの経路情報を有している場合、

前記ネットワークにアクセスするための 2 以上のインターフェース部と、

1 以上のネットワークからなるドメインを定義するドメイン定義部と、

ドメイン間における通信の可否を定義するドメイン間通信定義部と、

通信データの中継先を示す経路情報を前記ドメインごと区分して記憶する経路情報記憶部と、

通信データの中継を制御する中継制御部とを備え、

前記中継制御部は、同ドメイン内の中継においてはそのドメインに対応する経路情報記憶部を参照して通信データの中継を制御し、異なるドメイン間の中継においては前記ドメイン間通信定義部の定義に従い中継の可否を判定する通信データ中継装置。

【請求項 2】 前記通信データ中継装置は中継先ドメインに対する宛先アドレス検索部をさらに備え、中継元のドメインが中継先のドメインへの経路情報を有していない場合に、

前記宛先アドレス検索部は、中継元のドメイン内の送信元通信装置からの要求に対してその中継先のドメインへの宛先アドレスを検索し、その宛先アドレスに対応付けられる中継元ドメイン内の中継アドレスを送信元通信装置へ通知し、

前記中継制御部は、前記中継アドレス宛の通信データを前記中継先ドメインの宛先アドレスへ中継する請求項 1 記載の通信データ中継装置。

【請求項 3】 通信データを処理する通信データ処理装置を接続したドメインへの経路制御情報記憶部をさらに備え、

前記中継制御部は、通信データの中継を制御するときに、前記通信データ処理装置に通信データを処理させ、処理された通信データを中継する請求項 1 記載の通信データ中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークの中継装置に関する。

【0002】

【従来の技術】

（ドメインの概念）

従来からルーティングドメインとは、1以上のネットワークからなり、一つ以上の互いに協調する経路制御プロトコルにより管理され、その経路情報によりネットワーク層パケットが到達可能な範囲と定義されていた。例えば、インターネットはさまざまな経路制御プロトコルが動作している複数のネットワークから構成されている。このため、インターネットは1つのルーティングドメインである（以下ルーティングドメインを単にドメインと省略する）。

【0003】

今日まで、多くの企業が自社の情報インフラとしてインターネットの技術を用いた企業内網を構築してきた。こうしたネットワークにおいては、企業の秘密を守るため、あるいは外部からの妨害を避けるため、インターネットとの間にファイアウォール装置が配置されていた。このファイアウォール装置により、インターネットとの間の通信が監視・制限されていた。こうしたネットワークではセキュリティ上の理由から、企業内網の内部経路をインターネットに配布しないのが一般的であった。また、IPv4アドレスが不足しているため、企業内網でプライベートアドレスを用いるのが一般的であった。

【0004】

プライベートアドレスは企業ユーザが自由に利用できるインターネットアドレスの範囲である。しかし、インターネットにこれらの経路を配布することは禁止されていた。そのため、プライベートアドレスを使用する企業内網は、インターネットとは直接通信できなかった。したがって、企業内網はインターネットとは独立したドメインである。

【0005】

こうした企業内網が、インターネットと通信するためにはNAT (IP Network Address Translator) 装置を使用する必要があった。NAT装置は、プライベートアドレスを持つパケットをグローバルアドレスで経路制御されるインターネットに通すために、両ドメイン境界においてパケットに付されたプライベートアドレスをグローバルアドレスに変換する。

【0006】

さらに、企業内網構成の複雑化、ルータ機能の多様化に対応するため、ルータ装置がNAT機能を持つようになった（以下これをNATルータという）。このようなルータ装置は、二つのドメインを管理することができた。

【0007】

このような状況において、プライベートアドレスによるドメイン（以下プライベートアドレスドメインという）からグローバルアドレスによるドメイン（以下グローバルアドレスドメインという）への通信は、以下のように行われていた。

【0008】

すなわち、プライベートアドレスドメイン内の各ルータにおいて、宛先アドレスが企業内網内部以外であるパケットを全てNATルータへ送信するように、デフォルト経路が設定された。これにより、グローバルアドレスドメイン宛のパケットをドメイン境界に置かれた中継装置（以下ドメイン境界中継装置という）に送ることが可能であった。

【0009】

中継装置は、プライベートアドレスドメインの経路情報をグローバルアドレスドメインへ流さないが、グローバルアドレスドメインから得た経路情報をプライベートアドレスドメインへ流す。これにより、プライベートアドレスドメイン内の各ホスト（ノード）は、グローバルアドレスドメイン宛のパケットを中継装置に送ることが可能であった。

【0010】

ドメイン境界中継装置は、グローバルアドレスドメインから受け取った経路情報から、グローバルアドレスドメイン内の次ホップルータを知る（実際には、中継装置において、デフォルトルートとして外部ルータが指定してされている場合

もある)。こうして、ドメイン境界中継装置は、グローバルアドレスドメインへ向いたインタフェースへパケットを中継できた。このとき、実際にはドメイン境界中継装置は、中継する前にパケットのアドレスを変換した。

【0011】

アドレス変換にはいくつかの方法があった。例えば、まず、ドメイン境界に置かれた中継装置がグローバルアドレスをいくつかプールしておく。このドメイン境界中継装置は、到着したパケットのプライベートアドレスである送信元アドレスをプールしてあるグローバルアドレスの一つと置きかえる（以下このアドレスをエイリアスアドレスという）。

【0012】

次に、このドメイン境界中継装置が、あたかもグローバルアドレスドメイン内の送信ホストであるかのように送信する。このとき、ドメイン境界中継装置は、置き換えた送信元アドレスとそのエイリアスアドレスの対応を記録する。そして、ドメイン境界中継装置が、グローバルアドレスドメインから送信したパケットに対する応答トラフィックを受信したとき、プライベートアドレスドメイン内の本来の送信ホストへ中継する。

【0013】

また、プライベートアドレスドメインからグローバルアドレスドメインへ送信したパケットに対する応答パケットが返ってきた場合、宛先アドレスは上記エイリアスアドレスである。つまり、グローバルアドレスドメインにおいてはパケットの送信元が中継装置のエイリアスアドレスである。このため、ドメイン境界中継装置は、先のプライベートアドレスとグローバルアドレスとの変換テーブルを参照し、パケットの宛先アドレスをプライベートアドレスドメインの送信元アドレスに変換できる。こうして、ドメイン境界中継装置は、返信パケットをプライベートアドレスドメインへ接続されたインタフェースへと中継する。

【0014】

以上のようなアドレス変換機能により両ドメイン間の通信が可能であった。フォワード方向の通信では宛先ドメインにおける経路テーブルが必要であった。一方、プライベートアドレスとグローバルアドレスの変換テーブルにフォワード方

向パケットを受信したインタフェースも併せて記録しておけば、中継装置は、バックワードのパケットをその受信インターフェースへ転送すればよい。その際、送信元ドメインの経路情報を検索し、プライベートアドレスドメインにおける次ホップルータを決定し、上記インターフェースへ転送する。

【0015】

従来、ドメイン境界中継装置は、複数のルーティングプロトコルを終端する経路制御プログラムとただ一つの経路テーブルを有していた。なお、ここでいう経路テーブルとはパケット中継時に出力インタフェースと次ホップルータとを決定するために検索するテーブルを指す。

【0016】

従来の中継装置は、このような複数のルーティングプロトコルによって知り得た経路情報を相互に混合するか否かという管理上の制御を行っていた。しかし、相互に混合する場合、従来の中継装置では、このような複数のルーティングプロトコルから知り得た経路情報を全て同一の経路テーブルに書き込んでいた。つまり、プライベートアドレスドメインとグローバルアドレスドメイン境界の中継装置は、各ドメインから知り得た経路情報を一つのテーブル内で管理していた。

(Lucent Technologies社のIP Navigatorの例)

図19にLucent Technologies社のIP Navigatorの処理概要を示す。IP Navigatorは複数のルーティングテーブルをサポートする通信プログラムであった。IP navigatorはISP(Internet Service Provider)向けのMPLS(MultiProtocol Label Switching)プロトコルを実装する中継装置(以下ルータという)上で動作した。

【0017】

このIP navigatorは、LSR(ラベル・スイッチ・ルータ)において、複数の経路テーブル毎に、各ルータ間を接続するLSP(ラベル・スイッチ・パス)を対応付けることでISP(インターネット・サービス・プロバイダ)ネットワークをパーティションに分割した。そして、IP navigatorは、それぞれのパーティションを企業ユーザなどにプライベートネットワークとして提供することを目的としていた。この方式では複数のドメインに対してそれぞれ経路テーブルを持った。

ただし、この方式では、任意の組み合わせのドメインが互いにアドレス変換機能を介して、通信することはできなかった。

(IPv6ルータの実装)

現在まで、代表的なネットワーク層プロトコルとしてIPプロトコル (IPversion4、以下IPv4という) が用いられてきた。さらに、IPアドレスの枯渇に対応するため、IPプロトコルの新バージョン (IPversion6、以下IPv6という) が登場した。今日、IPv4とIPv6とは混在している。一般的には、このIPv4のドメインとIPv6のドメインとは、アドレス変換装置を用いて互いに通信する。両ドメインに対応するルータとして、IPv4経路テーブルを持つIPv4ドメインとIPv6の経路テーブルを持つIPv6ドメインとをアドレス変換により通信可能とするものがあった (株式会社日立製作所NR60など)。

【0018】

このようなルータは、IPv4,v6という二つのドメインに対しては複数の経路テーブルを持ち、両者の間でアドレス変換による通信が可能であった。しかし、ユーザがIPアドレス空間にさらにドメインを定義し、二つ以上のドメイン間をアドレス変換によって自由に接続することはできなかった。

(片方向NAT)

図20に片方向NATの概要を示す。片方向NATは、プライベートアドレスとグローバルアドレスのように、ドメイン1の経路情報をドメイン2に配布できないという条件下で通信を実現した。ドメイン1はドメイン2への経路を知り得るので、ドメイン1は、ドメイン2宛のパケットを中継可能である。

【0019】

NAT装置は、通過するパケットの送信元アドレスをドメイン2へ向いた自装置インタフェースのエイリアスアドレスに変換する。NAT装置は、アドレスを変換したパケットをドメイン2に送出するとともに、そのエイリアスアドレスと変換前の送信元アドレスを記憶する。

【0020】

これによりドメイン2内の受信ホストは、そのエイリアスアドレスに向けて応答パケットを送信する。すなわち、ドメイン2はドメイン1への経路は知らない

が変換されたNAT装置のエイリアスアドレスへは返信可能である。

【0021】

さらに、NAT装置は、このエイリアスアドレスで受信したパケットを記憶しておいたドメイン1側の本来の送信元アドレスへ向けて再送信する。

この場合、NAT装置の経路テーブルはドメイン1とドメイン2とを混合したテーブルであった。ドメイン2からドメイン1宛のパケットをフォーワーディングインタフェースで受けてしまうと経路テーブルを参照しフォワードされる可能性があった。このため、不正パケットに対するフィルタが必要であった。

(両方向NAT)

図21に両方向NATの概要を示す。両方向NATは、IPv4ドメインとIPv6ドメインのように、ドメイン1の経路情報もドメイン2の経路情報もお互いに交換できないという条件下で通信を実現した。ドメイン1内のホストがドメイン2内のホストへ通信を開始するとき、ドメイン1内のホストは通信に先だってDNSによる名前解決を実行する。

【0022】

ドメイン1内の解決要求はドメイン1内のDNSサーバを経由しNAT装置上の変換サーバでドメイン2内の解決要求に変換される。ドメイン2のDNSサーバから解決応答が戻ってくると、NAT装置はプールしてあるドメイン1とドメイン2とに向いたそれぞれのエイリアスアドレスを各インタフェースに設定する。そしてNAT装置は、ドメイン1の問い合わせホストにはこのドメイン1側のエイリアスアドレスを通知する。NAT装置は各エイリアスアドレスとドメイン2から受け取った解決アドレスの対応を記録しておく。

【0023】

送信ホストはNAT装置のドメイン1側のエイリアスアドレスへ向けてパケットを送信する。NAT装置は上記の対応を用いてヘッダの送信先アドレスを、解決応答によりドメイン2のDNSから得たアドレスに、送信元アドレスをドメイン2側のエイリアスアドレスに変更する。この場合、IPv4、v6のように全くアドレス体系が異なる場合は問題ない。しかし、両ドメインがIPv4アドレス空間の一部であるような構成において、NAT装置がエイリアスアドレス以外のインタフェースア

ドレスで悪意のあるパケットを受信した場合、フィルタが正しく設定されていないと、NAT装置は、このパケットをフォワードする可能性があった。

(アプリケーションゲートウェイ)

アプリケーションゲートウェイを使用してもドメインを分離可能であった。図 22 にアプリケーションゲートウェイの概要を示す。

【0024】

アプリケーションゲートウェイでは、一旦ゲートウェイ上のアプリケーションプログラム40がドメイン1からの通信を終端し、データを受け取る。さらに、このアプリケーションプログラム40は、ドメイン2側のコネクション上に再度データを送信する。この方式では、エンドホストが使うアプリケーションに対応したアプリケーションプログラム40をゲートウェイ上にも用意する必要があった。また、この方式では、処理が重いという問題点があった。

【0025】

(複数ドメインに対応したアドレス変換装置)

複数ドメインに対応した中継装置も提案されている。ただ、従来の中継装置には、単一の経路テーブルが備えられていた。また、ドメイン間でアドレス変換ポリシーに合致しないパケットが通過しないようにフィルタが用いられていた。単純な設定では、このような中継装置も利用できた。しかし、従来の中継装置では、管理ドメインが多数になると処理が複雑になった。また、全パケットについてドメイン間通信の判定を行う必要があった。

(問題点)

NAT等のアドレス変換の手法によれば、フォワード方向のパケット転送では、中継装置は、アドレス変換処理を施した後、経路テーブルを検索して転送を行う。中継装置は、パケットの送受信アドレスに対してフィルタを設定することで、パケットの中継の可否を判断してしていた。一方でバックワード方向のパケットに対しては、グローバルアドレスドメインに対し中継装置があたかも送信元ホストであるかのように振舞う。そして、中継装置は、エンドホストとして、中継装置にプールされていたグローバルアドレス宛のパケットを終端していた。

【0026】

同様に、グローバルアドレスドメインから到着したプライベートアドレスドメイン宛のパケットに対して、中継装置は、パケットフィルタによりドメイン間での中継判定を行っていた。このため、万が一プライベートアドレスドメイン宛の悪意のあるパケットが中継装置に到着した場合、フィルタが正しく設定されていないと、中継装置は唯一の経路テーブルを参照し、プライベートアドレスドメインにフォワードしてしまう可能性があった。これは予期せぬ不特定多数のパケットをインターネットから受信してしまう可能性を示しており、セキュリティホールとなり得た。

【 0 0 2 7 】

また、複数のドメインに接続可能な中継装置において、各ドメインが同一プライベートアドレス空間を採用した場合を想定する。この場合、中継装置が、各ドメインから得られた経路情報を一つの経路テーブルに書き込んでしまうと、経路テーブルに矛盾が生じる。

【 0 0 2 8 】

上記のような問題に対してパケットフィルタにより、グローバルアドレスドメインからのパケットをフォワードしないよう制限することも可能であった。しかし、管理可能なドメイン数が増加すると設定が複雑になった。

【 0 0 2 9 】

例えば、パケットフィルタでは、入力インターフェース、出力インターフェース、送信元アドレス、宛先アドレスやL4ポート番号等をキーとしてパケットの中継を制限可能であった。しかし、多くのインターフェースを持つルータでドメインを多数接続した場合、ドメインの組み合わせ毎にフィルタ条件を設定するのは煩雑であった。また、このような構成の中継装置では、設定ミスを誘発する可能性があった。さらに、このような複雑なフィルタ処理は、中継装置の負荷となり、高速な中継処理が困難であった。

【 0 0 3 0 】

【発明が解決しようとする課題】

本発明はこのような従来の技術の問題点に鑑みてなされたものであり、複数のドメイン間をアドレス変換によって中継する中継装置において、ドメイン間、ド

メイン内通信が混在している場合にも、ドメイン間では複雑なフィルタを設定せずにセキュリティを確保した通信を実行し、ドメイン内においては高速にパケットを中継することを技術的課題とする。

【 0 0 3 1 】

【課題を解決するための手段】

本発明は前記課題を解決するために、以下の手段を採用した。

すなわち、本発明は、1以上のネットワークを接続した、そのような2以上のドメイン間を中継する通信データ中継装置であって、中継元のドメインが中継先のドメインへの経路情報を有している場合、

ネットワークにアクセスするための2以上のインターフェース部と、

1以上のネットワークからなるドメインを定義するドメイン定義部と、

ドメイン間における通信の可否を定義するドメイン間通信定義部と、

通信データの中継先を示す経路情報を前記ドメインごと区分して記憶する経路情報記憶部と、

通信データの中継を制御する中継制御部とを備えたものである。この通信データ中継装置において、中継制御部は、同一ドメイン内の中継においてはそのドメインに対応する経路情報記憶部を参照して通信データの中継を制御し、異なるドメイン間の中継においては前記ドメイン間通信定義部の定義に従い中継の可否を判定する。

【 0 0 3 2 】

この通信データ中継装置は、中継先ドメインに対する宛先アドレス検索部をさらに備え、中継元のドメインが中継先のドメインへの経路情報を有していない場合に、宛先アドレス検索部は、中継元のドメイン内の送信元通信装置からの要求に対してその中継先のドメイン内の宛先アドレスを検索し、その宛先アドレスに対応付けられる中継元ドメイン内の中継アドレスを送信元通信装置へ通知する。

【 0 0 3 3 】

中継制御部は、中継アドレス宛の通信データを中継先ドメインの宛先アドレスへ中継することができる。

この宛先アドレス検索部とは、例えば通信装置のネットワーク上の名称からそ

のアドレスを検索するものをいう。この宛先アドレス検索部は、他の通信装置に宛先アドレスの検索を依頼するものであってもよい。

【 0 0 3 4 】

この通信データ中継装置は、通信データを処理する通信データ処理装置を接続したドメインへの経路制御情報記憶部をさらに備え、

前記中継制御部は、通信データの中継を制御するときに、この通信データ処理装置に通信データを処理させ、処理された通信データを中継するようにしてもよい。ここで、通信データ処理装置とは、例えば通信データの内容をチェックする装置である。

【 0 0 3 5 】

【発明の実施の形態】

以下、本発明の好適な実施の形態を図面を参照して説明する。

(第 1 実施形態)

以下、本発明の第 1 実施形態を図 1 から図 1 2 の図面に基いて説明する。

【 0 0 3 6 】

図 1 は第 1 実施形態におけるネットワーク構成図であり、図 2 は図 1 に示したルータ 3 のハードウェア構成図であり、図 3 は、このルータ 3 の機能構成図であり、図 4 及び図 5 は、図 2 に示した CPU 1 4 で実行される制御プログラムの処理を示すフローチャートであり、図 6 から図 1 2 は CPU 1 4 が取り扱うデータのデータ構造を示す図である。

<ネットワークの構成>

図 1 に第 1 実施形態におけるネットワーク構成図を示す。図 1 のように、本実施形態においては、ルータ 3 がイントラネット A、イントラネット B、イントラネット C、及びインターネットを接続している。図 1 のようにルータ 3 は、各ネットワークを論理的なインターフェース de0、de1、de2、及び、de3を介して接続する（インターフェース部に相当）。

【 0 0 3 7 】

イントラネット A のプライベートアドレスは、10.25.165.0/24である。イントラネット A は、単独でドメイン 1 を構成している。イントラネット A は、ルータ

3のインターフェースde1に接続されている。このイントラネットAは、ルータ3においてアドレス変換されることにより、インターネットと接続可能である。

【0038】

イントラネットBのプライベートアドレスは、192.168.0.0/16である。このイントラネットBには、通信装置192.168.5.1が接続されている。イントラネットBは、ルータ3のインターフェースde2に接続されている。このイントラネットBもルータ3を介してインターネットと接続可能である。

【0039】

イントラネットCのプライベートアドレスは、192.172.0.0/16である。イントラネットCは、ルータ3のインターフェースde3に接続されている。このイントラネットCもルータ3を介してインターネットと接続可能である。また、上記イントラネットBとイントラネットCとは、ドメイン2を構成する。

【0040】

インターネットは、グローバルアドレスでアクセスされる。また、インターネットには、ネットワーク4と、ネットワーク5とが接続されている。さらに、インターネットは、ルータ3のインターフェースde0に接続されている。

【0041】

ネットワーク4のグローバルアドレスは、100.10.5.0/24である。また、ネットワーク4には、通信装置100.10.5.2が接続されている。

ネットワーク5のグローバルアドレスは、150.10.23.0/24である。また、ネットワーク5には、通信装置150.10.23.5が接続されている。

【0042】

以上のインターネット、ネットワーク4及びネットワーク5は、ドメイン0を構成している。

図1に示した各ドメインは相互にネットワーク層での到達性がない独立した経路制御を行っている。さらに本実施形態においては、ドメイン2からドメイン0及び1に対して、アドレス変換を行うことで接続が許可されている。また、ドメイン1からドメイン2への通信は許可されていない。ドメイン1からドメイン0へは、アドレス変換を行うことで接続が許可されている。

<ルータ 3 のハードウェア構成>

図 2 に本実施形態に係るルータ 3 のハードウェア構成図を示す。

【 0 0 4 3 】

このルータ 3 は、制御プログラムやデータを記憶するメモリ 1 3 と、メモリ 1 3 に記憶された制御プログラムを実行する CPU 1 4 と、CPU 1 4 から制御されて他の通信装置と通信する複数の物理インターフェース 1 5 a、1 5 b、1 5 c とを備えている。

【 0 0 4 4 】

メモリ 1 3 は、CPU 1 4 が実行する制御プログラムや CPU 1 4 が処理するデータを記憶する。

CPU 1 4 は、メモリ 1 3 に記憶された制御プログラムを実行し、中継装置 1 としての機能を提供する。

【 0 0 4 5 】

物理インターフェース 1 5 a、1 5 b、1 5 c は、CPU 1 4 からの指令により通信データをネットワーク 1 0 に送出し、またはネットワークから通信データを受信する。

<機能構成>

図 3 にルータ 3 の機能の構成図を示す。CPU 1 4 は、中継制御プログラム 3 1 と経路制御プログラム 3 0 とを実行することによりルータ 3 の機能を提供する。また、中継制御プログラム部分は、CPU によらず、ハードウェアにより構成してもよい。

【 0 0 4 6 】

中継制御プログラム 3 1 は、パケット受信部 2 8、経路検索部 2 5、ドメイン間通信判定部 2 6、アドレス変換部 2 7、及びパケット送信部 2 9 からなる。この中継制御プログラム 3 1 を実行する CPU 1 4 が中継制御部に相当する。

【 0 0 4 7 】

一方、CPU 1 4 は、上記中継制御プログラム 3 1 とは、別に経路制御プログラム 3 0 を実行している。これにより、CPU 1 4 は、他の通信装置及び他のルータとの間で経路情報を交換する。

[宛先ドメイン経路テーブル20]

宛先ドメイン経路テーブル20は、宛先ネットワークに対応する送信先インターフェース（以下送信インターフェースという）を登録したテーブルである。

【0048】

図8、図9及び図10に、各々ドメイン0、ドメイン1及びドメイン2を宛先とする宛先ドメイン経路テーブル20の例を示す。本実施形態において、宛先ドメイン経路テーブル20は、例えば、図8に示すように宛先ネットワークのアドレス、次ホップゲートウェイのアドレス、及びその宛先ネットワークに対応する送信インターフェースを識別する情報を有している。

【0049】

また、図8、図9及び図10に示すように、本実施形態では宛先ドメイン経路テーブル20は、宛先ドメインごとに独立したテーブル構造を有する。

CPU14は、パケットを中継する際に宛先ドメイン経路テーブル20を参照し、出力インターフェースを決定する。

[受信インターフェースドメイン経路テーブル21]

受信インターフェースドメイン経路テーブル21は、パケットを受信したインターフェース（以下受信インターフェースという）に対応するドメインの経路情報を格納する。この受信インターフェースドメイン経路テーブル21と上記宛先ドメイン経路テーブル20とが経路情報記憶部に相当する。

[ドメイン定義テーブル22]

ドメイン定義テーブル22は、各インターフェースに対応するドメインを定義したテーブルである（ドメイン定義部に相当）。図6に本実施形態におけるドメイン定義テーブル22の定義例を示す。

【0050】

図6のように、本実施形態においては、ドメイン定義テーブル22はインターフェースを識別する情報（インターフェース番号）とドメインを識別する情報（ドメイン番号）とを有している。例えば、インターフェース番号de0に対応するドメインは、ドメイン0である。

【0051】

なお、インターフェースとしては、物理的なインターフェースだけでなく、論理的なインターフェースを登録してもよい。

[ドメイン間通信定義テーブル 23]

ドメイン間通信定義テーブル 23 は、ドメイン定義テーブル 22 で定義した各ドメインに対して、他のドメインとの接続の可否を定義したテーブルである（ドメイン間通信定義部に相当）。図 7 に本実施形態におけるドメイン間通信定義テーブル 23 の定義例を示す。

【0052】

図 7 のように、ドメイン間通信定義テーブル 23 は、送信元ドメイン→宛先ドメインの指定、そのドメイン間の通信の可否、及び、変換ルール（アドレス変換の方式）の組み合わせからなるレコードで構成される。本実施形態における設定では、例えば、ドメイン 0 からドメイン 1 及びドメイン 2 への通信は許可されない。また、ドメイン 2 からドメイン 0 及び 1 への通信は許可され、かつ、変換ルールとして NAT が適用される。

[アドレス変換テーブル 24]

アドレス変換テーブル 24 は、アドレス変換前後の情報を対にしたレコードからなるテーブルである。図 11 に本実施形態におけるアドレス変換テーブル 24 の例を示す。

【0053】

図 11 のように、アドレス変換テーブル 24 は変換前後の送信元アドレス、宛先アドレス及び送受信インターフェースを 1 組にしたレコードから構成される。これらの情報は、送信元から宛先へのパケットが中継装置 1 を最初に通過するときに設定される。その後、2 つ目以降のパケットの通信においては、アドレス変換テーブル 24 が参照される。

[経路検索部 25]

経路検索部 25 は、パケットの宛先アドレスをキーとして、経路テーブルを検索する。

[ドメイン間通信判定部 26]

ドメイン間通信判定部 26 は、パケットヘッダ情報やネームサービス（通信装

置のホスト名称に対応するアドレスを示すプログラム)等を用いて、宛先の通信装置がどのドメインに属するか判定する。

[アドレス変換部 2 7]

アドレス変換部 2 7 は、ドメイン間通信判定部 2 6 から、変換前後の情報(送信元アドレス、宛先アドレス)を受ける。この情報に従い、アドレス変換部 2 7 は、パケットのヘッダ内容を変換する。

[パケット受信部 2 8]

パケット受信部 2 8 は、物理インターフェース 1 5 a 等を監視する。そして、パケット受信部 2 8 は、物理インターフェース 1 5 a 等に接続したネットワークからパケットを受信する。

[パケット送信部 2 9]

パケット送信部 2 9 は、物理インターフェース 1 5 a 等を制御し、物理インターフェース 1 5 a 等に接続したネットワークへパケットを送信する。

[経路制御プログラム 3 0]

経路制御プログラム 3 0 は、経路制御プロトコルを実行する。すなわち、経路制御プログラム 3 0 は、ドメイン内に流れる経路情報 1 0 2 を受信し、受信した経路情報 1 0 2 に合わせて自ルータの経路テーブルを変更する。また、経路制御プログラム 3 0 は、自ルータから同ドメイン内の他ルータへのネットワーク到達性情報や接続コスト等を経路情報 1 0 2 に入れて、他ルータへ配布する。本実施形態では経路制御プログラム 3 0 はドメイン毎に個別用意する。各経路制御プログラム 3 0 は、各々対応するドメインと経路情報を交換する。その結果得られたドメインごとの経路情報は、宛先ドメインごとに宛先ドメイン経路テーブル 2 0 に保存される。

【 0 0 5 4 】

なお、経路制御プロトコルとしては、RIP(Routing Information Protocol、インターネットに関するドキュメント RFC1058 参照)、OSPF(Open Shortest Path First、RFC1131 参照)等が知られている。

<機能概要>

以下図 3 に従い、ルータ 3 の機能概要を説明する。

(1) ルータ 3 はパケット受信部 28 により宛先ホストを指定されたパケット 100 を受信する。

(2) まず、経路検索部 25 は、受信インタフェースが属するドメインへの経路テーブル（受信インターフェースドメイン経路テーブル 21）を検索する。受信インターフェースドメイン経路テーブル 21 の検索がヒットした場合、経路検索部 25 は、ドメイン内ルーティングとして中継する。すなわち、経路検索部 25 はパケット送信部 29 に指示し、出力インタフェースにパケットを出力させる。

【0055】

受信インタフェースドメイン経路テーブル 21 の検索がヒットしない場合、(3) 以下に示す手順が実行される。

(3) ドメイン間通信判定部 26 は、受信したパケットのヘッダ情報、受信インタフェースなどをキーとしてアドレス変換テーブルを順引き、逆引きで検索する。順引き、逆引きのどちらかで検索がヒットした場合は、ドメイン間通信判定部 26 は、アドレス変換手段にパケットを渡す。

【0056】

検索がヒットしない場合、ドメイン間通信判定部 26 は、パケットのヘッダ情報、宛先ドメイン経路テーブル 20 及びドメイン定義テーブル 22 から受信したパケットの宛先アドレスがどのドメインに属するかを調べる。次に、ドメイン間通信判定部 26 は、ドメイン定義テーブル 22 に登録された受信インタフェースが属するドメインを調べる。次に、ドメイン間通信判定部 26 は、ドメイン間通信定義テーブル 23 を参照し、受信インタフェースが属するドメインと宛先ドメインとの間の通信の可否を判断する。なお、ドメイン間通信定義テーブル 23 にはアドレス変換ルールも示されている。

(4) ドメイン間通信判定部は、受信インタフェースが属するドメインと宛先ドメインとの通信が可能な場合は、宛先ドメイン経路テーブル 20 を参照するよう経路検索部 25 に通知する。

(5) 経路検索部 25 は、ドメイン間通信判定部 26 から起動され、宛先ドメイン経路テーブル 20 を検索する。この検索では、パケットヘッダ情報の宛先アドレスをキーとして使用する。

(6) アドレス変換部 27 はパケットに対しドメイン間通信定義テーブル 24 に記された変換ルールに従いパケットヘッダ情報を変換する。

(7) パケット送信部 29 は、検索された出力インタフェースにパケットを出力する。

(8) 経路制御プログラム 30 は各ドメイン毎に起動し、各ドメインへの宛先ドメイン経路テーブル 20 及び受信インターフェースドメイン経路テーブル 21 を修正する。

<通常処理>

以下に、本実施形態におけるネットワーク間の接続条件を示す。

〔接続条件 1〕 イントラネット A(10.25.165.0) はルータ 3 によりアドレス変換されることでインタネットと通信可能である。

〔接続条件 2〕 イントラネット B(192.168.0.0) はルータ 3 を通してブランチオフィスであるイントラネット C(192.172.0.0) と接続される。

〔接続条件 3〕 イントラネット B, C は共にルータ 3 を介してインターネットに接続可能である。

【 0 0 5 7 】

図 4 及び図 5 に上記接続を実現するための中継制御プログラム 31 の処理を示す。この中継制御プログラム 31 は、CPU 14 において実行される。

まず、順方向の通信（送信元通信装置から宛先通信装置へのパケット送信）に対する処理を説明する。

(1) ルータ 3 でのパケット受信

今、ルータ 3 が、インターフェース de2 を介して、ドメイン 2 に属するネットワーク 192.168.100.0 からパケットを受信した場合の処理を説明する。このパケットの宛先アドレスは、100.10.5.2、送信元アドレスは、192.168.5.1 である。

(2) 自局宛てパケット判定

まず、ルータ 3 の CPU 14 は、このパケットがルータ 3 そのものへ宛てられた（以下自局宛てという。自局宛を自ノード宛ともいう）パケットか否かを判定する（ステップ S1、以下 S1 と略す）。自局宛てパケットは、ルータ 3 自身への通信パケットとして処理される（S3）。

【0058】

本実施形態では、自局宛てパケットは、ルータ3への環境設定パケットである。この環境設定パケットは、ネットワーク管理者がルータ3にリモートログインすることで発せられる。ルータ3の環境設定そのものに関する説明は省略する。

【0059】

今、パケットは、環境設定パケットではないため、S2の判定は、Noである。従って、CPU14は、処理をドメイン内通信判定（S4）に進める。

（3）ドメイン内通信判定

次に、CPU14は、このパケットが同一ドメイン内の宛先に宛てられているか否かを判定する（S4）。この判定では受信インタフェースが属するドメイン宛の宛先経路テーブル（受信インターフェースドメイン経路テーブル21）を検索する。その検索がヒットした場合は（S5の判定でYesの場合）、受信インタフェースに対応する送信元ドメインと宛先ドメインとが同一であることを意味する。すなわち、同一ドメイン内でパケットを中継すればよい（S6）。

【0060】

ヒットしなかった場合（S5の判定でNoの場合）は、ドメイン間通信判定部26に処理を渡す（S7）。この例では、同一ドメイン内の通信でないため、CPU14は制御をS7の処理に進める。

（4）ドメイン間通信判定部26、アドレス変換部27、及びパケット送信部29の処理

ドメイン間通信判定部26では、受信したパケットの宛先アドレス、送信元アドレスをキーとして図11のアドレス変換テーブル24を検索する。アドレス変換テーブル24の検索がヒットした場合は（S8の判定でYesの場合）、検索結果とともにパケットがアドレス変換部27に送られる（S9）。これは順方向通信でアドレス変換すべきパケットであることを示している。アドレス変換部27では、与えられた検索結果を元にパケットのヘッダを書き換える。また、CPU14は、アドレス変換テーブル24（図11）から送信インターフェースを求める。

【0061】

次に、CPU14は、パケット送信部29に制御を移し、パケットを上記送信インターフェースからネットワークに送信する(S11)。

この検索がヒットしない場合は(S8の判定でNoの場合)、CPU14は、図5に示す処理に制御を移す。すなわち、CPU14は、パケットの宛先アドレスをアドレス変換テーブル24における変換後の送信元アドレスとして、パケットの送信元アドレスをアドレス変換テーブル24における変換後の宛先アドレスとして、アドレス変換テーブル24を検索する(S12)。

【0062】

ここで、検索がヒットした場合は(S13の判定でYesの場合)、CPU14は、パケットが順方向通信に対する応答通信(逆方向通信)のパケットであると判断する。そこで、CPU14は、検索された内容と共にパケットをアドレス変換部27に渡す。さらにCPU14は、アドレス逆変換を指示する(S14)。その結果、CPU14は、パケットの宛先をアドレス変換テーブルにおける変換前の送信元アドレスに書き換える。また、CPU14は、アドレス変換テーブル24から返信先インターフェース(図11の受信インターフェース)を求める。

【0063】

次に、CPU14は、パケット送信部29に制御を移し、パケットを上記送信インターフェースからネットワークに送信する(S16)。

どちらにもヒットしない場合は(S13の判定でNoの場合)、CPU14は、ドメインをまたがる通信を行うかどうかを判断する(S17及びS18の処理)。これは新たにドメイン間通信を開始する場合に必要な処理である。

【0064】

すなわち、CPU14は、宛先アドレスをキーとして宛先ドメイン経路テーブル20の全体を検索して、送信インターフェースを求める。

今、宛先アドレスが、100.10.5.2であるので、CPU14は、送信インターフェースとしてde0を得る。次にCPU14は、この送信インターフェースをキーとしてドメイン定義テーブル22を検索して宛先ドメインを求める。今、送信インターフェースがde0であるので、CPU14は、宛先ドメインとしてドメイン0を得る。さらに、CPU14は、受信インターフェースをキーとして、ドメイン

定義テーブル 22 を検索する。CPU 14 は、パケットを受信したインタフェース番号とドメイン定義テーブル 22 (図 6) とから、CPU 14 は、送信元ドメインとしてドメイン 2 を得る (S 17)。

【0065】

次に、CPU 14 は、得られた送信元ドメイン及び宛先ドメインをキーとして、図 7 のドメイン間通信定義テーブル 23 を検索する (S 18)。

今、この検索はヒットするので (S 19 で Yes の場合)、両ドメインの接続が許可されていることが分かる。また、NAT によるアドレス変換が指定されていることが分かる。

【0066】

本実施例形態で実現する NAT では送信元アドレスのみが変換される。この変換には、宛先ドメインごとにプールされている IP アドレスが使用される

このとき、CPU 14 は、図 11 のアドレス変換テーブル 24 に、変換前のアドレスと変換後のアドレスを対応させて登録する (S 20)。

【0067】

また、CPU 14 は、受信インターフェース、送信インターフェースもアドレス変換テーブル 24 に登録する (S 21)。

次に、CPU 14 は、パケット送信部 29 に制御を移し、パケットを上記送信インターフェースからネットワークに送信する (S 22)。

【0068】

S 18 の判定において、2 つのドメイン間の接続が不許可の場合は (S 19 の判定で No の場合)、CPU 14 は、パケットを廃棄する (S 23)。

<効果>

以上によれば順方向、逆方向ともにドメイン間通信判定部 26 により許可されたパケットのみが宛先ドメイン経路テーブル 24 を参照可能となるため、悪意のあるパケットを誤って中継してしまうことを回避できる。

【0069】

また、本実施形態のルータ 3 では、宛先ドメインごとに経路テーブルを分離し、かつ、パケットを受信した段階で受信インターフェースドメイン経路テーブル 2

1 を優先的に参照する。このため、受信インターフェースに対応するドメイン宛の packets (同ドメイン内の宛先に対する packets) に対しては、経路テーブルの検索は、そのドメインに対応する経路テーブル (受信インターフェースドメイン経路テーブル 21) に限定される。その結果、同ドメイン宛 packets の中継が効率化される。

【0070】

一方、インターネットからイントラネットに侵入する悪意のある packets を排除するためのドメイン間通信判定部 26 の処理は、上記のような同ドメイン宛以外の packets に対して実行すればよい。

<変形例>

上記第 1 実施形態においては、宛先ドメイン経路テーブル 20 と受信インターフェース経路テーブル 21 とが異なるテーブルとして構成された。しかし、本発明の実施は、このような構成に限定されるものではない。例えば、受信インターフェース経路テーブル 21 を宛先ドメイン経路テーブル 20 の一部として構成してもよい。ただし、上記第 1 実施形態と同様に、宛先ドメイン経路テーブル 20 は、各宛先ドメイン毎に論理的に独立したテーブル構造を有するものとする。

【0071】

この場合は、packets 受信部で packets を受信した際、packets を受信したインターフェースをキーとして、ドメイン定義テーブルを検索し、受信ドメインを決定し、適するドメイン経路テーブルを選択する。

【0072】

上記第 1 実施形態では、経路制御プログラム 30 は、各宛先ドメイン毎に個別に用意した。しかし、本発明の実施は、このような構成には、限定されない。例えば、1 つの経路制御プログラム 30 (経路制御プロトコルを実行する CPU 14 上の 1 つのプロセス) を備えてもよい。その場合、このプログラムが宛先ドメインごとに経路情報を交換する処理を順次繰り返すようにすればよい。

【0073】

上記第 1 実施形態では、ルータ 3 は、論理的なインターフェース de0、de1、または de2 をドメインに対応付けた。しかし、本発明の実施は、このような構成に

は、限定されない。例えば、論理的なインターフェース 15a 等を使用せず、直接物理インターフェース 15a、15b、または 15c を各ドメインに対応付けてもよい。この場合は、物理インターフェース 15a 等がインターフェース部に相当する。

【0074】

上記実施形態においては、宛先ドメイン経路テーブル 20 は、図 8 から図 10 のように宛先ドメインごとに分離して構成した。しかし、本発明の実施は、このような構成に限定されない。例えば、図 12 に示したように単一のテーブルで宛先ドメイン経路テーブル 20 を構成しても、テーブルを構成するレコードが宛先ドメインごとに分離されていればよい。

【0075】

上記実施形態の中継装置 1 では、ドメイン間で最初に通信されるパケットの宛先アドレスに基づき、全ての宛先ドメイン経路テーブルの全体を検索して出力インターフェースを求めた。そして、その出力インターフェースから宛先ドメインを決定し、送信元ドメインと宛先ドメインとのドメイン間の接続の可否を判定した（図 5 の S17 及び S18 の処理）。しかし、本発明の実施はこのような処理手順には限定されない。すなわち、宛先ドメイン経路テーブル間で、アドレスに重複がある場合を考慮し、S18 の処理を先に行ってもよい。まず、ドメイン間通信定義テーブル 23 を検索し、通信が許可されている受信ドメインを決定しておく。そして、そのような通信が許可されているドメインの経路テーブルのみを検索し、出力インターフェースを求めることも可能である（図 5 において S18 の処理を先に実行し、S17 の処理を後から実行することに相当する）。

（第 2 実施形態）

図 13 から図 17 を参照して、本発明の第 2 実施形態を説明する。図 13 は、本実施形態のネットワーク構成図であり、図 14 は本実施形態に係るルータ 3 の機能構成図であり、図 15 は、ルータ 3 の CPU 14 で実行されるアドレス事前登録部 25 の処理を示すフローチャートであり、図 16 はアドレス事前登録部 25 の処理結果を示す図であり、図 17 はルータ 3 の CPU 14 で実行される中継制御プログラム 31 の処理を示す図である。

【0076】

上記第1実施形態では、宛先ドメイン経路テーブル20及び受信インターフェースドメイン経路テーブル21を備えたルータ3を説明した。この場合、上記第1実施形態では、ドメイン2においては、ドメイン0への経路が既知であった。

【0077】

本実施形態では、ルータ3に接続される2つのドメインにおいて互いに相手の経路が不明である場合の中継処理を説明する。ただし、送信元ドメインは相手ドメインのホスト名から相手ドメイン内のアドレスを知る手段があるものとする。他の構成及び作用については、第1形態と同様であるので、同一の構成については、同一の符号を付してその説明を省略する。また、必要に応じて図1から図12の図面を参照する。

<構成>

図13に本実施形態に係るネットワーク構成図を示す。本実施形態では、互いに相手への経路が不明なドメイン0とドメイン2とを接続するルータ3を説明する。

【0078】

図13のようにドメイン0には、sub1.0の名称で示されるネットワーク4が含まれている。また、ネットワーク4には、ホスト名n0.sub1.0のホストが接続されている。このホストn0.sub1.0のアドレスは、100.10.5.2である。

【0079】

また、ドメイン2には、アドレス192.168.5.1で示されるホストが接続されている。ドメイン0とドメイン2とは、互いに相手ドメインへの経路が不明である。ただし、本実施形態では、ドメイン2のホスト192.168.5.1は、宛先ホストのホスト名n0.sub1.0を知っているものとする。

【0080】

このような場合、本実施形態においては、送信元ホスト192.168.5.1は、ルータ3に対して宛先の名称に対応するアドレスを問い合わせることができる。

図14に本実施形態におけるルータ3の機能構成を示す。図14の構成は、アドレス変換事前登録部25（アドレス検索部に相当）が追加されている点で、図

3 に示した第 1 実施形態の構成と相違する。

【 0 0 8 1 】

アドレス変換事前登録部 2 5 は、事前にアドレス変換テーブル 2 4 に変換前後の情報を登録する機能を有する。

＜アドレス変換事前登録部 2 5 における処理＞

以下、送信元ホスト 192.168.5.1 が、ルータ 3 に宛先のホスト名称に対応する宛先アドレスを問い合わせた場合の処理を説明する。

【 0 0 8 2 】

図 1 5 にルータ 3 の CPU 1 4 が実行するアドレス変換事前登録部 2 5 の処理を示す。まず、CPU 1 4 は、ネームサービス (RFC 9 2 1) を実行する不図示のサーバにその宛先のホスト名称 n0.sub1.0 に対応するドメイン 0 内のアドレスを問い合わせる (S 4 1)。その結果、CPU 1 4 は、宛先ホストのアドレス 10.0.10.5.2 を得る。

【 0 0 8 3 】

次に、CPU 1 4 は、宛先ホストのドメイン番号 0 に基づき、宛先ドメインごとに区分された宛先ドメイン経路テーブル 2 0 を検索し、出力インターフェース de0 を求める (S 4 2)。

【 0 0 8 4 】

次に CPU 1 4 は、上記第 1 実施形態と同様に受信インターフェース de2 の属するドメイン 2 を求める (S 4 3)。

次に CPU 1 4 は、2 つドメイン間の接続可否 (ドメイン 2 からドメイン 0 への接続可否) をドメイン間通信定義テーブル 2 3 に従って判定する (S 4 4)。2 つのドメイン間の通信が認められない場合 (S 4 4 の判定で No の場合)、ルータ 3 は、その旨を送信元 192.168.5.1 へ通知する (S 4 5)。

【 0 0 8 5 】

一方、ドメイン 2 からドメイン 0 への通信が認められる場合 (S 4 4 の判定で Yes の場合)、CPU 1 4 は、予めプールしておいたドメイン 2 におけるエイリアスアドレス 192.168.5.2 を求める (S 4 6) (以下、このエイリアスアドレスを受信インターフェースアドレスと呼ぶ)。また、CPU 1 4 は、予めプールし

ておいたドメイン 0 におけるエイリアスアドレス 120.10.4.2 を求める（以下、このエイリアスアドレスを送信インターフェースアドレスと呼ぶ）。

【 0 0 8 6 】

そして、CPU 1 4 は、送信元アドレス 192.168.5.1、受信インターフェースアドレス 192.168.5.2、受信インターフェース de2、送信インターフェースアドレス 120.10.4.2、宛先アドレス 100.10.5.2、送信インターフェース de0 をアドレス変換テーブル 2 4 に登録する（S 4 7）。この登録された結果を図 1 6 に示す。

【 0 0 8 7 】

次に、ルータ 3 は、送信元 192.168.5.1 に対し、本受信インタフェースアドレス 192.168.5.2 を予め通知する（S 4 8）。これによって、送信元 192.168.5.1 は、その受信インタフェースアドレス 192.168.5.2 にパケットを送信すれば、所望の宛先ホスト n0.sub1.0 にパケットを送信できることを知る。

【 0 0 8 8 】

以上の処理は、通信に先だって、送信元 192.168.5.1 とルータ 3 との間で実行される。このような設定の後、上記受信インターフェースアドレス 192.168.5.2 宛のパケットを受信したルータ 3 は、アドレス変換テーブル 2 4 に従い、宛先をアドレス 100.10.5.2 に変換し、出力インターフェース de0 から送信する。この結果パケットは、ドメイン 2 からドメイン 0 に中継される。

<受信インターフェースアドレスによる接続処理>

図 1 7 に受信インターフェースアドレスによる接続処理のフローチャートを示す。この処理は、ルータ 3 の CPU 1 4 が、中継制御プログラム 3 1 として実行する。

（１）パケット受信

今、ルータ 3 が、インターフェース de2 を介して、ドメイン 2 に属するネットワーク 192.168.0.0 からパケットを受信した場合の処理を説明する。このパケットの宛先アドレスは、192.168.5.2（上記受信インターフェースアドレス）、送信元アドレスは、192.168.5.1 である。

（２）自局宛てパケット判定

まず、ルータ 3 の CPU 1 4 は、このパケットが自局宛てパケットか否かを判

定する（S 1）。

【0 0 8 9】

本実施形態で、自局宛てパケットとは、ルータ 3 自身へのへの環境設定パケット、または上記通知した受信インターフェースアドレス宛のパケットである。

今、パケットは、受信インターフェースアドレス宛のパケットであるため、S 2 の判定は、Yes である。従って、CPU 1 4 は、制御を S 3 1 以下の処理に進める。

（3）自局あてパケット処理

次に、CPU 1 4 は、送信元アドレス 192.168.5.1 と宛先アドレス 192.168.5.2 とをキーにしてアドレス変換テーブル 2 4 を検索する（S 3 1）。

【0 0 9 0】

上記 2 つのアドレスの組み合わせは、アドレス変換テーブル 2 4 に登録済みであるので（図 1 6 参照）、この検索はヒットする（S 3 2 の判定で Yes となる）。そこで CPU 1 4 は、S 3 3 以下の処理に制御を進める。

【0 0 9 1】

すなわち、CPU 1 4 は、アドレス変換部 2 7 を実行する（S 3 3）。その結果、受信インターフェースアドレス 192.168.5.2 に対応するドメイン 0 内の宛先アドレス 100.10 5.2 及び送信インターフェース de0 が求められる。

【0 0 9 2】

次に CPU 1 4 は、パケット送信部 2 9 を実行し、上記宛先 100.10 5.2 に送信インターフェース de0 からパケットを送信する。

（4）パケット返信処理

上記宛先 100.10 5.2 からの返信パケットの処理は、第 1 実施形態で説明した図 5 のフローチャートの S 1 2 から S 1 6 の処理と同様であるので、その説明を省略する。

【0 0 9 3】

以上のように互いに経路情報を交換しない 2 つのドメイン間に対しても、ルータ 3 にアドレス変換事前登録部 2 5 を備えることで本発明の実施は可能である。

また、本実施形態のルータ 3 では、宛先ドメイン経路テーブル 2 0 を宛先ドメ

インごとに分離して構成する。従って、複数のドメイン間でプライベートアドレスが重複する場合でも、アドレス事前登録部 2 5 は、適切な出力インターフェースを宛先ドメイン経路テーブル 2 0 から求めることができる。

＜変形例＞

上記第 2 実施形態においては、互いに経路情報を交換しない 2 つのドメイン間を接続するルータ 3 を説明した。しかし、本発明の実施は、このようなドメイン間の接続に限定されない。すなわち、中継される 2 つのドメインの一方のみが、他方への経路情報を有していない場合にも本発明は同様に実施できる。つまり、中継先ドメインへの経路情報を有していないドメインから中継先へ通信する場合に、第 2 実施形態で説明したルータ 3 は、上記同様にパケットを中継できる。

（第 3 実施形態）

上記第 1 実施形態では、宛先ドメイン経路テーブル 2 0 及び受信インターフェースドメイン経路テーブル 2 1 を備えたルータ 3 を説明した。

【 0 0 9 4 】

本実施形態では、上記第 1 実施形態の構成において、アドレス変換部 2 7 の提供する機能の一部（コンテンツチェック）を他のドメイン上のサーバ（通信データ処理装置に相当）に実行させるルータ 3 について説明する。

【 0 0 9 5 】

図 1 8 を参照して、本発明の第 3 実施形態を説明する。図 1 8 は、本実施形態に係るルータ 3 の機能構成図である。図 1 8 は、サーバドメイン経路テーブル 3 1 及びコンテンツチェックサーバ 3 2 が付加されている点で第 1 実施形態の図 3 と相違する。他の構成及び作用については、第 1 実施形態及び第 2 実施形態と同様であり、同一の構成については、同一の符号を付してその説明を省略する。また、必要に応じて、図 1 から図 1 7 の図面を参照する。

【 0 0 9 6 】

図 1 8 のように、本実施形態のルータ 3 の CPU 1 4 は、サーバへの経路情報を保持するサーバドメイン経路テーブル 3 1 を備えている。CPU 1 4 は、このサーバドメイン経路テーブル 3 1 を検索する。この検索結果に従い、CPU 1 4 は中継するパケットのアドレスをコンテンツチェックサーバ 3 2 宛に変換して送

信する。次にCPU14は、コンテンツチェックが終わったパケットを受信する。次にCPU14は、そのパケットをアドレス逆変換し、本来の宛先ドメインへアドレス変換する。

【0097】

このようにコンテンツチェックをコンテンツチェックサーバ32に実行させることにより、ルータ3の負荷が低減され、高速な中継処理が実現される。

【0098】

【発明の効果】

以上説明したように、本発明によれば、1以上のネットワークを接続した、そのような2以上のドメイン間を中継する通信データ中継装置であって、

1以上のネットワークからなるドメインを定義するドメイン定義部と、

ドメイン間における通信の可否を定義するドメイン間通信定義部と、

通信データの中継先を示す経路情報を前記ドメインごと区分して記憶する経路情報記憶部とを備え、同一ドメイン内の中継においてはそのドメインに対応する経路情報記憶部を参照して通信データの中継を制御し、異なるドメイン間の中継においては前記ドメイン間通信定義部の定義に従い中継の可否を判定する。従って、ドメイン間、ドメイン内通信が混在している場合にも、ドメイン内においては高速にパケットを中継し、ドメイン間では複雑なフィルタを設定せずにセキュリティを確保した通信を実行することができる。

【図面の簡単な説明】

【図1】 本発明の第1実施形態におけるネットワーク構成図

【図2】 本発明の第1実施形態におけるルータのハードウェア構成図

【図3】 本発明の第1実施形態におけるルータの機能構成図

【図4】 制御プログラムの処理を示すフローチャート(1)

【図5】 制御プログラムの処理を示すフローチャート(2)

【図6】 ドメイン定義テーブルのデータ構造を示す図

【図7】 ドメイン間通信定義テーブルのデータ構造を示す図

【図8】 宛先ドメイン経路テーブルのデータ構造を示す図(1)

【図9】 宛先ドメイン経路テーブルのデータ構造を示す図(2)

- 【図 1 0】経路テーブルのデータ構造を示す図 (3)
- 【図 1 1】アドレス変換テーブルのデータ構造を示す図
- 【図 1 2】実際の経路テーブルのデータ構造例を示す図
- 【図 1 3】本発明の第 2 実施形態におけるネットワーク構成図
- 【図 1 4】本発明の第 2 実施形態におけるルータの機能構成図
- 【図 1 5】アドレス事前登録部の処理を示すフローチャート
- 【図 1 6】アドレス事前登録部によるアドレス変換テーブルへの登録結果
- 【図 1 7】受信インターフェースアドレスによる中継処理を示すフローチャート

ト

- 【図 1 8】本発明の第 3 実施形態におけるルータの機能構成図
- 【図 1 9】従来技術 L S P (ラベル・スイッチ・パス) の概要
- 【図 2 0】従来技術片方向 N A T の概要
- 【図 2 1】従来技術両方向 N A T の概要
- 【図 2 2】従来技術アプリケーションゲートウェイの概要

【符号の説明】

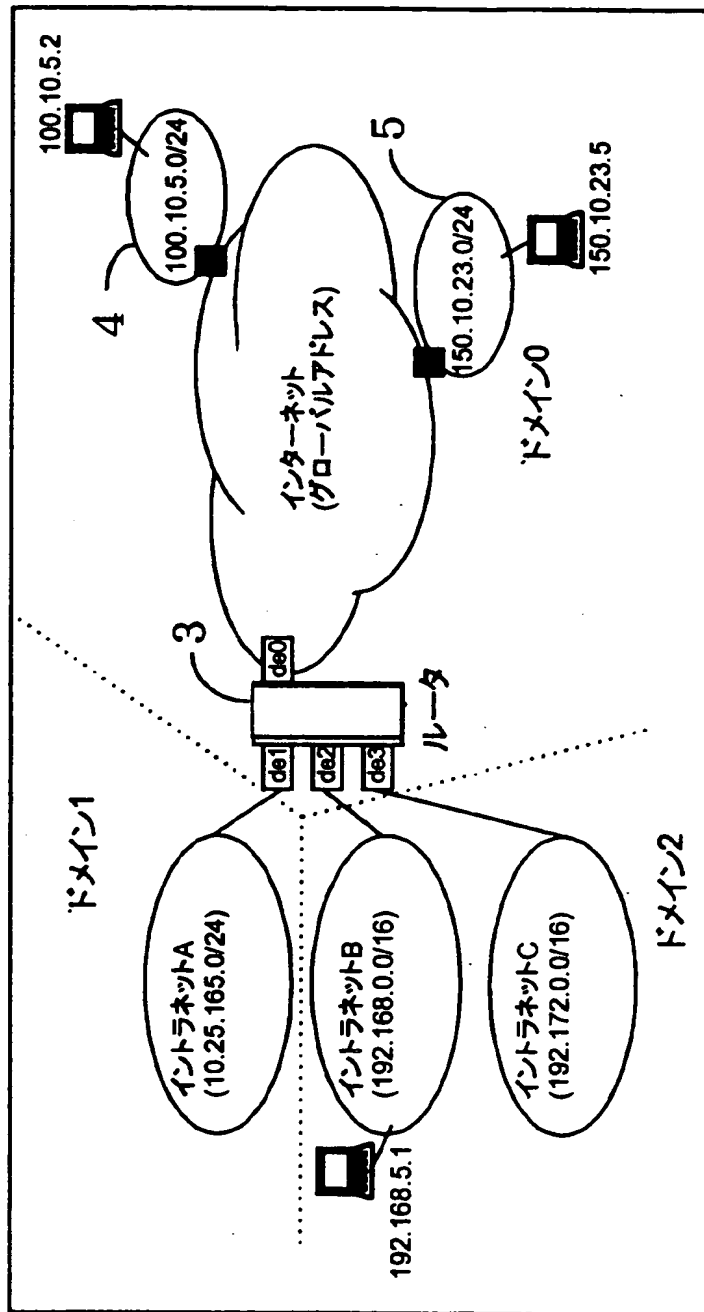
- 3 ルータ
- 1 3 C P U 1
- 1 4 メモリ
- 1 5 a 物理インターフェース
- 1 5 b 物理インターフェース
- 1 5 c 物理インターフェース
- 2 0 宛先ドメイン経路テーブル
- 2 1 受信インターフェース経路テーブル
- 2 2 ドメイン定義テーブル
- 2 3 ドメイン間通信定義テーブル
- 2 4 アドレス変換テーブル

【書類名】

図面

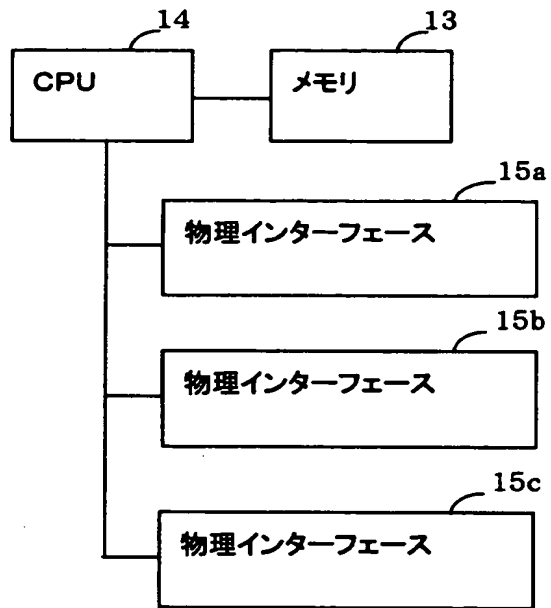
【図 1】

第1実施形態のネットワーク構成図



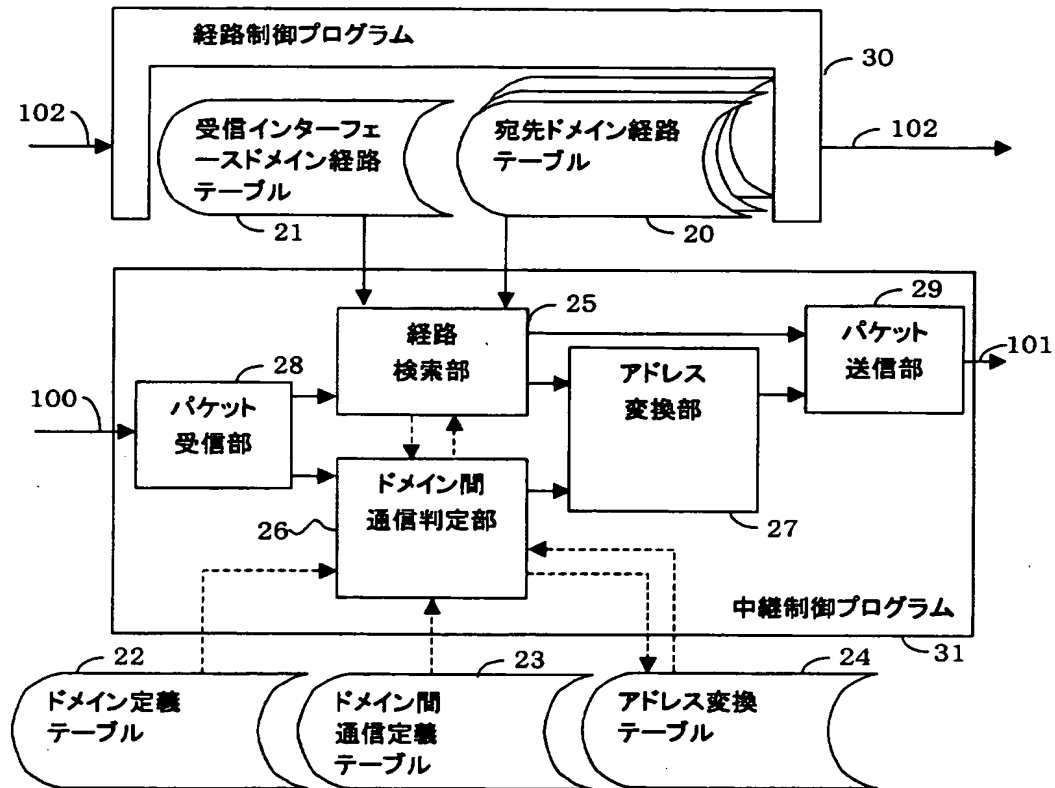
【図 2】

ルータ3のハードウェア構成図



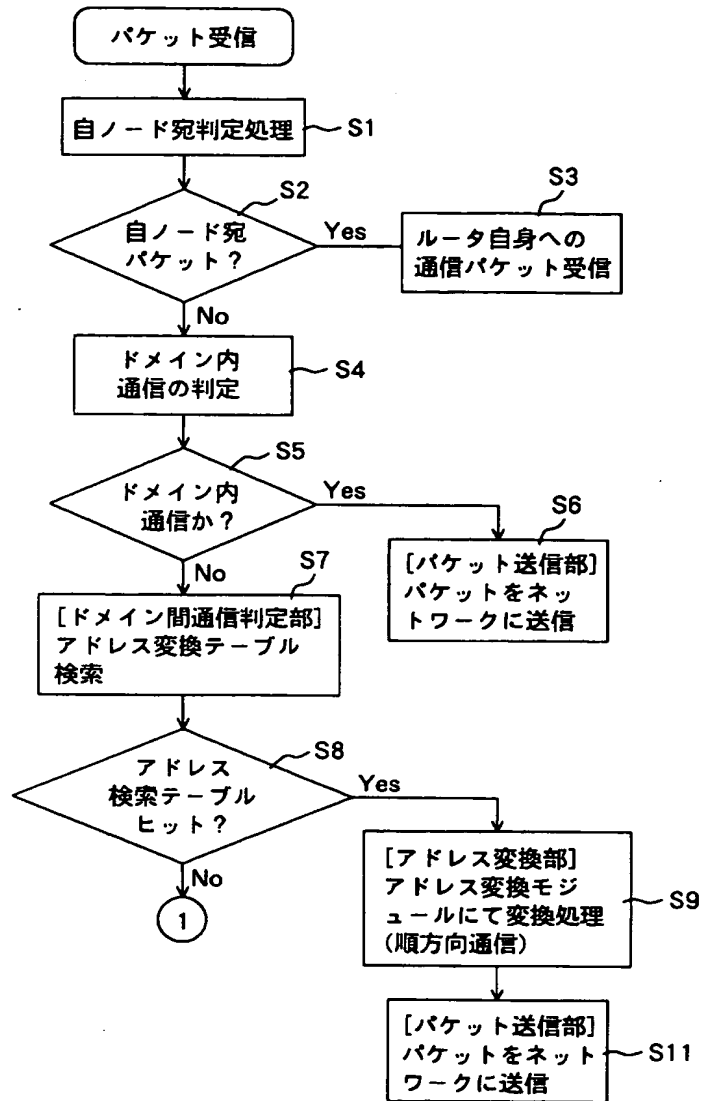
【図 3】

第1実施形態におけるルータ3の機能構成図



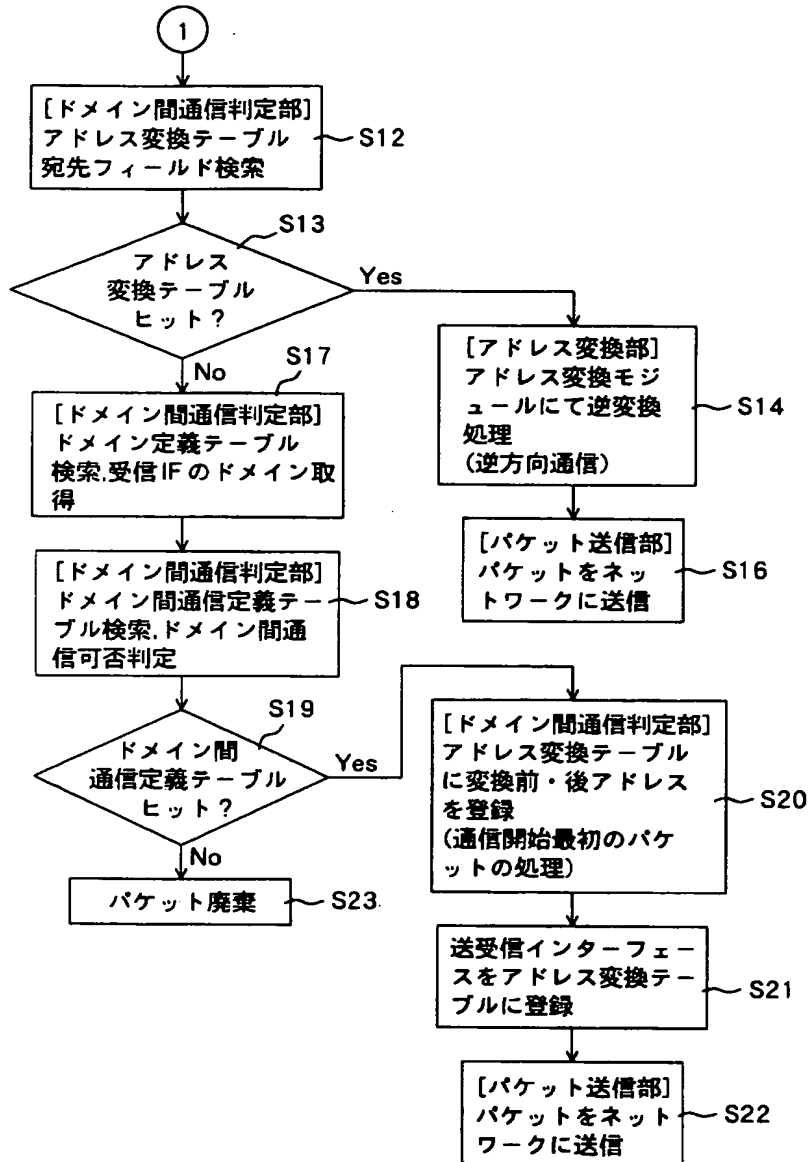
【図 4】

第1実施形態における中継装置の処理 (1)



【図 5】

第1実施形態における中継装置の処理 (2)



【図 6】

ドメイン定義テーブルの例

I/F 番号	ドメイン番号
de0	0
de1	1
de2	2
de3	2

【図 7】

ドメイン間通信定義テーブルの例

送信元ドメイン→宛先ドメイン	通信の可否 (1:許可 0:不許可)	変換ルール
ドメイン 0→ドメイン 1	0	-
ドメイン 0→ドメイン 2	0	-
ドメイン 1→ドメイン 0	1	NAT
ドメイン 1→ドメイン 2	0	-
ドメイン 2→ドメイン 0	1	NAT
ドメイン 2→ドメイン 1	1	NAT

【図 8】

宛先ドメイン 0 に対する宛先ドメイン経路テーブル

宛先ネットワーク	次ホップゲートウェイ	出力インタフェース
100.10.5.0	120.10.4.1	de0
100.10.6.0	120.10.4.120	de0
120.10.4.0	120.10.4.120	de0

【図 9】

宛先ドメイン 1 に対する宛先ドメイン経路テーブル

宛先ネットワーク	次ホップゲートウェイ	出力インタフェース
10.25.55.0	10.25.55.1	de1
10.25.165.0	10.25.55.165	de1
10.25.166.0	10.25.55.166	de1

【図 1 0】

宛先ドメイン 2 に対する宛先ドメイン経路テーブル

宛先ネットワーク	次ホップゲートウェイ	出力インタフェース
192.168.100.0	192.168.100.1	de2
192.168.250.0	192.168.100.250	de2
192.168.251.0	192.168.100.251	de2
192.172.30.0	192.168.30.1	de3
192.172.38.0	192.168.30.38	de3

【図 1 1】

アドレス変換テーブルの例

変換前			変換後		
送信元 アドレス	宛先 アドレス	受信 I/F	送信元 アドレス	宛先 アドレス	送信 I/F
192.168.5.1	100.10.5.2	de2	120.10.4.2	100.10.5.2	de0
192.172.3.1	100.10.6.7	de3	120.10.4.3	100.10.6.7	de0

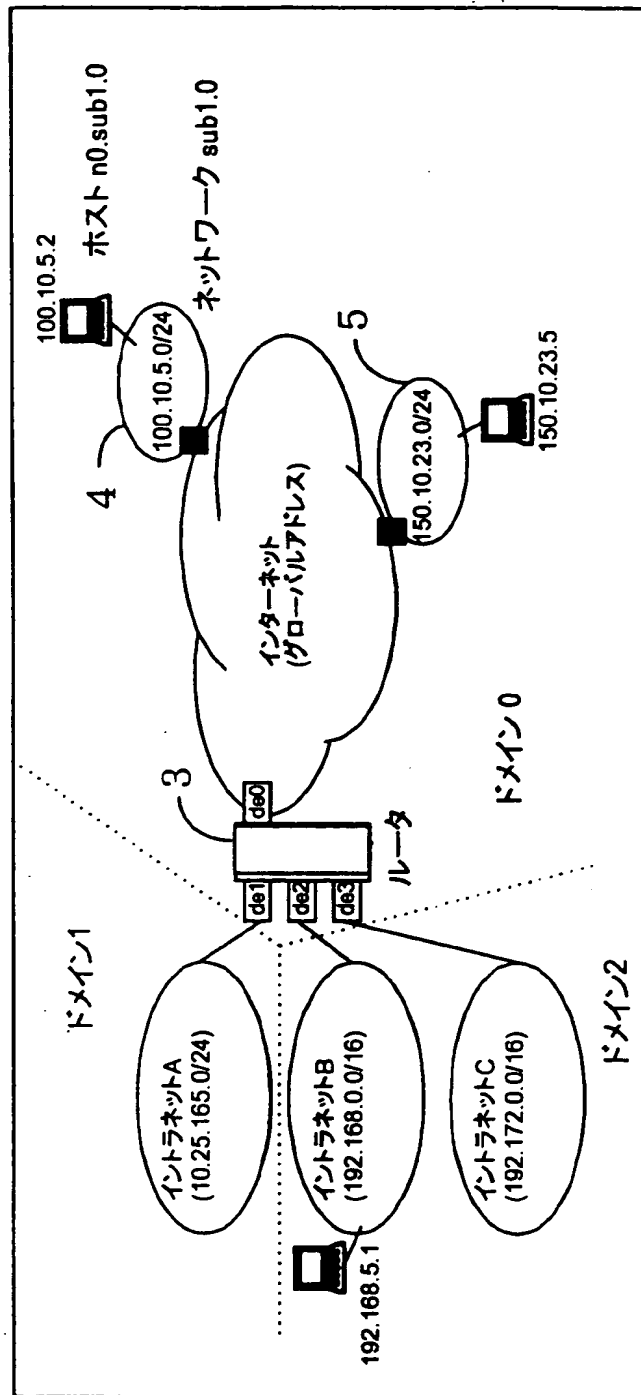
【図 1 2】

経路テーブルの例

宛先 ネットワーク	次ホップ ゲートウェイ	出力 インタフェース	ドメイン番号
100.10.5.0	120.10.4.1	de0	0
100.10.6.0	120.10.4.120	de0	0
120.10.4.0	120.10.4.120	de0	0
10.25.55.0	10.25.55.1	de1	1
10.25.165.0	10.25.55.165	de1	1
10.25.166.0	10.25.55.166	de1	1
192.168.100.0	192.168.100.1	de2	2
192.168.250.0	192.168.100.250	de2	2
192.168.251.0	192.168.100.251	de2	2
192.172.30.0	192.168.30.1	de3	2
192.172.38.0	192.168.30.38	de3	2

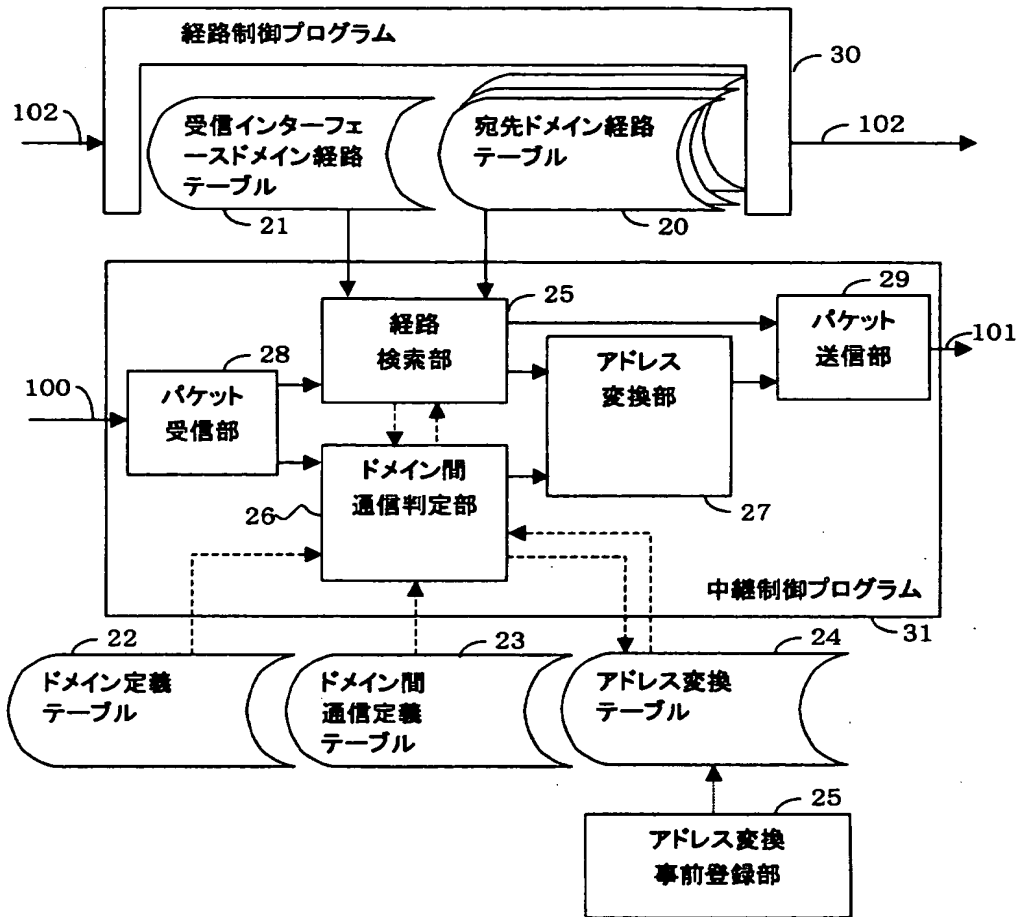
【図13】

第2実施形態のネットワーク構成図



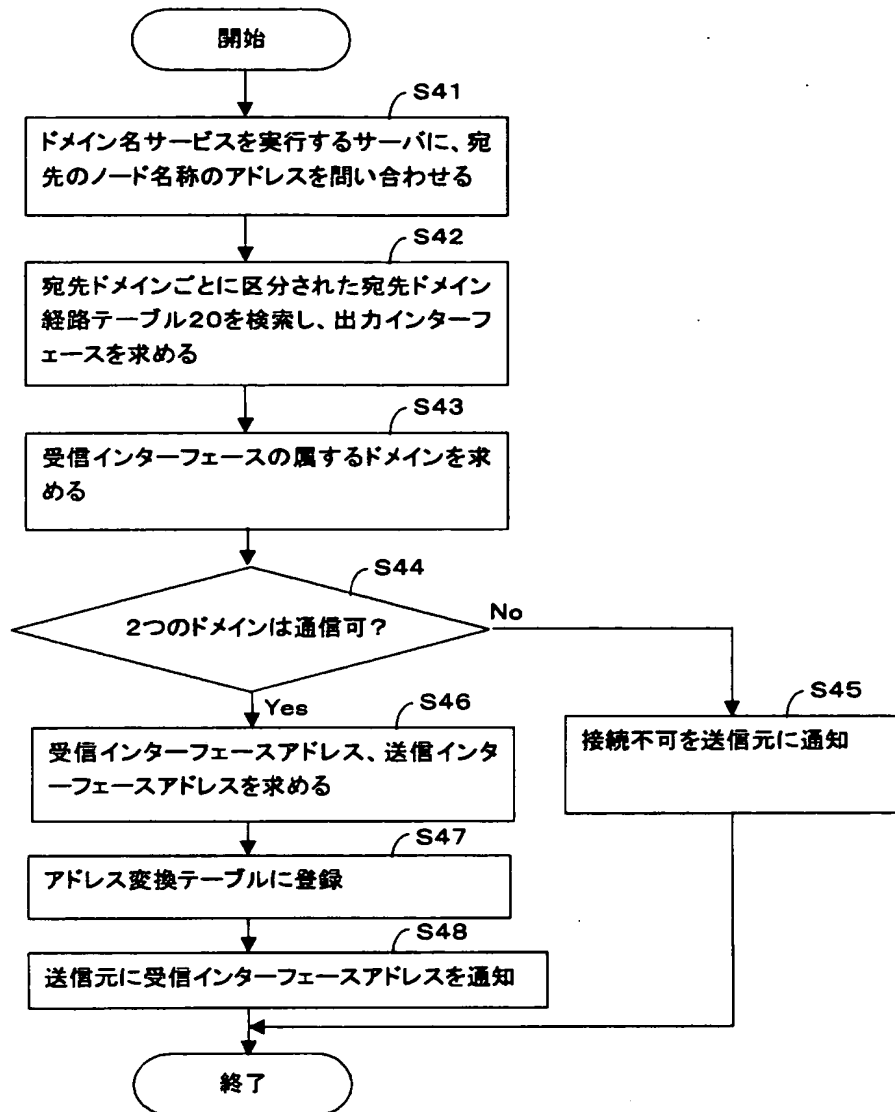
【図 14】

第2実施形態におけるルータ3の機能構成図



【図 15】

アドレス事前登録部の処理



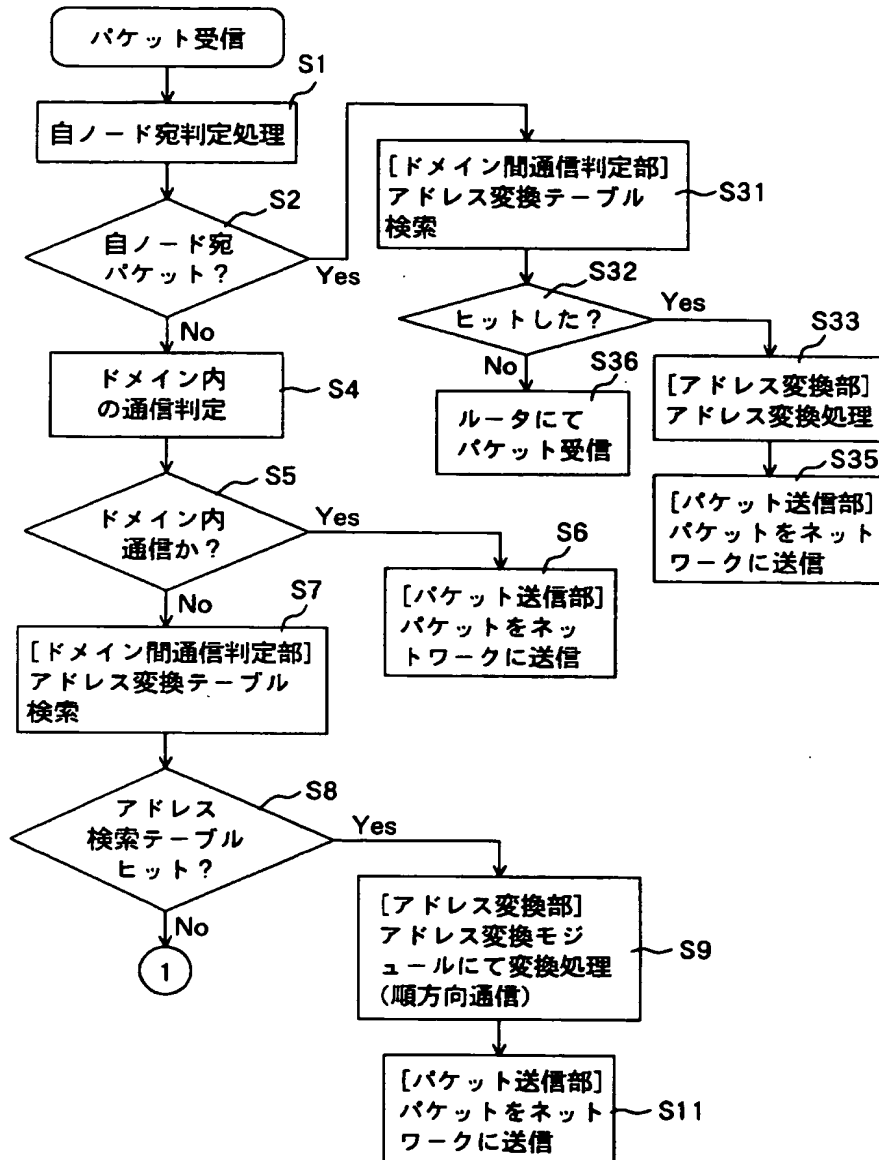
【図 1 6】

アドレス事前登録部によるアドレス変換テーブルへの登録結果

変換前			変換後		
送信元 アドレス	宛先 アドレス	受信 I/F	送信先 アドレス	宛先 アドレス	送信 I/F
192.168.5.1	192.168.5.2	de2	120.10.4.2	100.10.5.2	de0

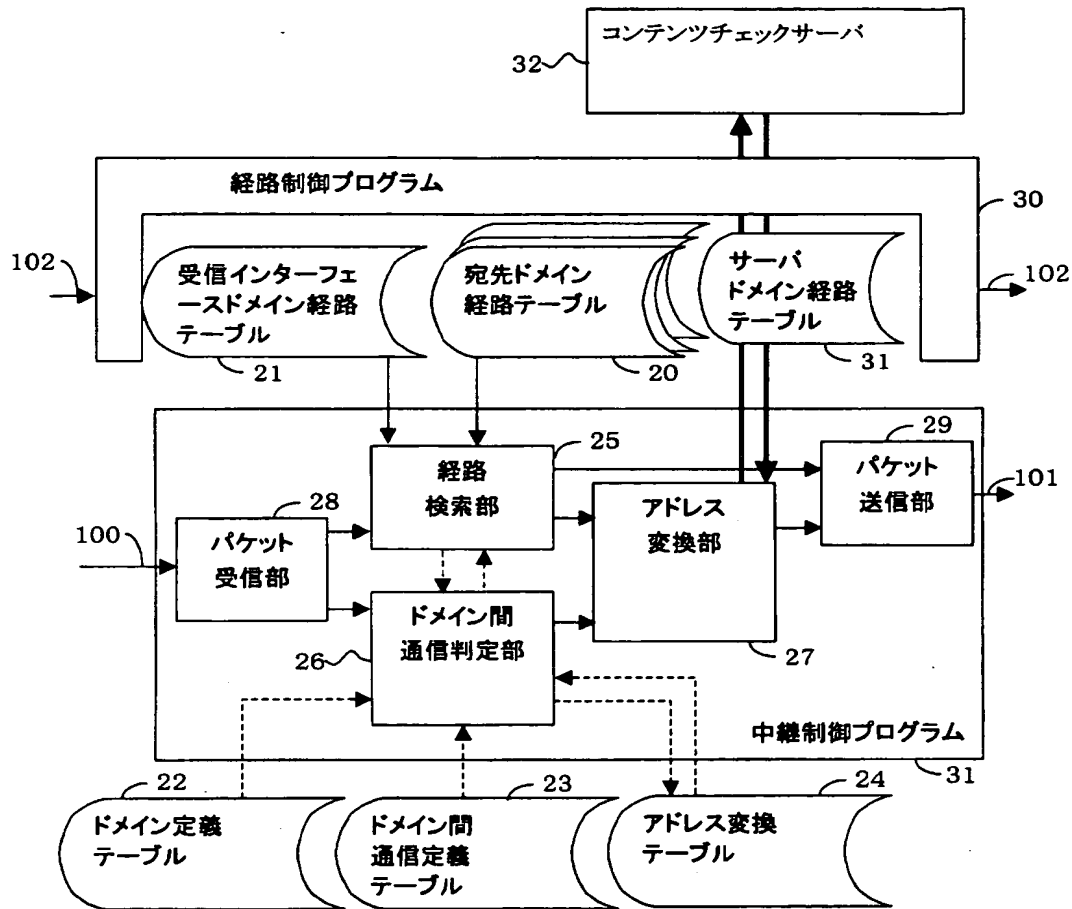
【図 17】

受信インターフェースアドレスによる中継処理



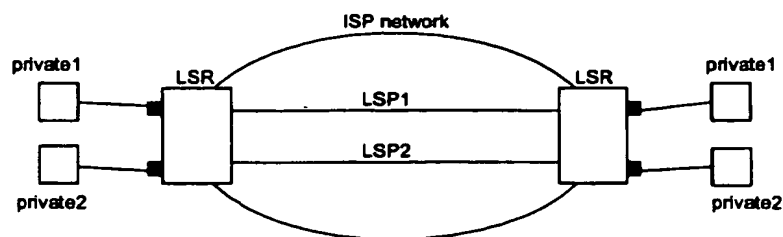
【図 18】

第3実施形態におけるルータ3の機能構成図



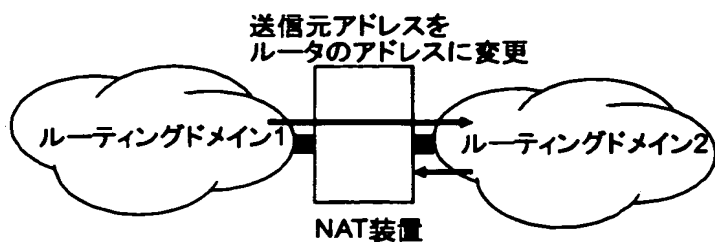
【図 19】

LSP (ラベル・スイッチ・パス) の概要



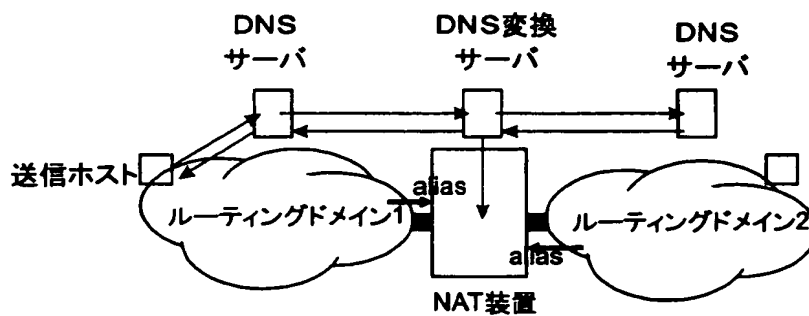
【図 20】

片方向 NAT の概要



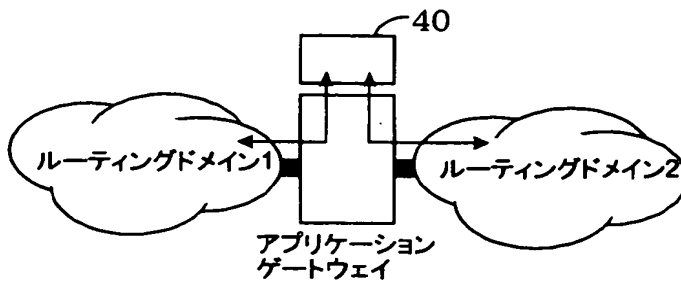
【図 21】

両方向 NAT の概要



【図 2 2】

アプリケーションゲートウェイの概要



【書類名】 要約書

【要約】

【課題】本発明は、複数のドメイン間をアドレス変換によって中継する中継装置において、ドメイン間、ドメイン内通信が混在している場合にも、ドメイン間では複雑なフィルタを設定せずにセキュリティを確保した通信を実行し、ドメイン内においては高速にパケットを中継することを技術的課題とする。

【解決手段】本発明は、1以上のネットワークを接続した、そのような2以上のドメイン間を中継する通信データ中継装置であって、中継元のドメインが中継先のドメインへの経路情報を有している場合、

ネットワークにアクセスするための2以上のインターフェース部と、

1以上のネットワークからなるドメインを定義するドメイン定義部と、

ドメイン間における通信の可否を定義するドメイン間通信定義部と、

通信データの中継先を示す経路情報を前記ドメインごと区分して記憶する経路情報記憶部と、

通信データの中継を制御する中継制御部とを備えたものである。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社